Claim

1. A method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link, wherein Mobile Terminal (MT) and Access Point (AP) perform the two-way certificate authentication through the Authentication Server (AS); and MT and AP perform negotiation of secret key for conversation.

2. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

when MT logs on AP, MT and AP performs said two-way certificate authentication through AS;

after said two-way certificate authentication is successfully performed, MT and AP perform said negotiation of the secret key for conversation.

3. Said method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

when MT logs on AP, MT and AP inform one another of their respective certificate, and then they perform negotiation of secret key for conversation;

after said negotiation of secret key for conversation is completed, MT and AT performs the two-way certificate

authentication through AS, and meanwhile judge whether the certificate used by the other part is the same as the one informed by it. If it is not, the authentication fails; if it is, the result of the authentication depends on the result of said two-way certificate identification.

4. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claims 1, 2 or 3, wherein: said two-way certificate authentication comprising the steps:

1) when MT logs on AP, MT sends to AP the access authentication request message containing the MT certificate;

2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing the AS signature;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT the certificate authentication response message as the access authentication response message; and

5) after MT receives said access authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete said two-way certificate identification between MT and AP.

5. Said method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, MT sends to AP the access authentication request message containing the MT certificate for said two-way certificate authentication;

2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate for said two-way certificate authentication, and meanwhile begins with MT negotiation of the secret key for conversation;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends

back to MT the certificate authentication response message as the access authentication response message for said two-way certificate authentication; and

5) after MT receives said access authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete the process of said two-way certificate identification between MT and AP, and then MT performs the corresponding processing to complete said negotiation of secret key for conversation.

6. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, MT sends AP the access authentication request message containing the MT certificate for said two-way certificate authentication;

2) after AP receives said access authentication request message, it adds the AP certificate to the message, then sends to AS the certificate authentication request message containing said MT certificate and AP certificate for said two-way certificate authentication;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate. AP judges the result of authentication. If the authentication is not successful, AP sends back to MT said certificate authentication response message as the access authentication response message for said two-way certificate authentication; If the authentication is successful, AP begins to consult with MT the secret key for conversation while it sends back to MT said access authentication response message; and

5) after MT receives said certificate authentication response message, MT authenticates the AS signature and obtains the result of authentication of the AP certificate, so as to complete said two-way certificate identification between MT and AP, and then MT performs the corresponding processing to complete said process of negotiation of secret key for conversation.

7. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, wherein:

1) when MT logs on AP, each part informs the other of its own certificate, then they complete said negotiation of secret key for conversation, and, meanwhile, MT also completes informing AP of the access authentication request identification;

2) AP sends to AS the certificate authentication request message containing the MT certificate and AP certificate for said

two-way certificate authentication;

3) after AS receives said certificate authentication request message, AS authenticates the AP certificate and MT certificate in said message, and then sends back to AP the certificate authentication response message containing AS signature for said two-way certificate authentication;

4) after AP receives said certificate authentication response message, AP authenticates the AS signature, so as to obtain the result of authentication of the MT certificate, and then sends back to MT said certificate authentication response message as the access authentication response message for said two-way certificate authentication; and

5) after MT receives said access authentication response message, MT authenticates the AS signature, and then judges whether the AP certificate is the same as the one AP informed of before negotiation of secret key for conversation. If it is not, the authentication fails; if it is, MT obtains the result of the authentication of the AP certificate from the message, so as to complete said two-way certificate authentication process between MT and AP.

8. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 4, 5 or 6 wherein: said access authentication request message also comprising the access authentication request identification.

9. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 4, 5, 6 or 7, wherein: said certificate authentication request message also comprising the access authentication request identification, or also comprising the access authentication request identification and AP signature.

10. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 4, 5, 6 or 7, wherein: said certificate authentication response message also comprising, before the signature filed of AS, the information of the result of the MT certificate authentication and those of the AP certificate authentication.

11. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 4, 5, 6 or 7, wherein: said access authentication response message is identical with said certificate authentication response message.

12. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 7, 8, or 9 wherein: said access authentication request identification is a string of random data or authentication serial number.

13. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data

communication via wireless link according to claim 10 or 11, wherein: said information of MT certificate authentication result comprising the MT certificate, and the MT certificate authentication result and the AS signature, or comprises the MT certificate and the MT certificate authentication result.

14. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 10 or 11, wherein: said information of the AP certificate authentication result comprises the AP certificate, the AP certificate authentication result, the access authentication request identification and the AS signature, or comprises the AP certificate, the AP certificate authentication result and the access authentication request identification.

15. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, 2, 3, 5, 6 or 7, wherein: when MT intends to access to the designated AP, the MT must first of all obtain the relevant information of the AP or the certificate of the AP.

16. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, 2, 3, 5, 6 or 7, wherein: said negotiation of secret key for conversation refers to MT or AP using AP's or MT's common key and their respective own private key to generate the secret key for conversation.

17. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, 2, 3, 5, 6 or 7, wherein: said negotiation of secret key for conversation comprising:

1) MT secretly chooses an integer a, from which to calculate the integer f(a), combines the integer f(a) and the MT signature on it into the secret key negotiation request message, and transmits it to AP; said f is a function rendering integer a from the integer f(a) incalculable;

2) after it receives said secret key negotiation request message, AP secretly chooses an integer b, from which to calculate the integer f(b), combines the integer f(b) and the AP signature on it into the secret key negotiation response message, and transmits it to MT; said f is a function rendering integer b from the integer f(b) incalculable; and

3) AP calculates g(b,f(a)), and MT calculates g(a, f(b)) after it receives said secret key negotiation response message, as the secret key for conversation in the process of communication; said g is a function rendering the calculation of g(a, f(b))=g(b,f(a)) possible.

18. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, 2, 3, 5, 6 or 7, wherein: said negotiation of secret key for conversation comprising:

1) AP secretly chooses an integer b, from which to calculate integer f(b), combines the integer f(b) and the AP signature on it into the secret key negotiation request message, and transmits it to MT; said f is a function rendering integer a from the integer f(b) incalculable;

2) after it receives said secret key negotiation request message, MT secretly chooses an integer a, from which to calculate the integer f(a), forms the integer f(a) and the MT signature on it into the secret key negotiation response message, and transmits it to AP; said f is a function rendering integer a from the integer f(a) incalculable; and

3) MT calculates g(a,f(a)), and AP calculates g(a, f(b)) after it receives said secret key response message, as the secret key for conversation in the process of communication; said g is a function rendering the calculation of g(a, f(b))=g(b,f(a)) possible.

19. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, 2, 3, 5, 6 or 7, wherein: said negotiation of secret key for conversation comprising:

1) MT or AP generates a string of random data, and sends them to AP or MT as the secret key negotiation request message after encryption using the common key of AP or MT;

2) After it receives said secret key negotiation request

message from MT or AP, AP or MT uses its own private key for decryption, obtains the random data generated by the other part; then AP or MP generates again a string of random data; and sends them to MT or AP as the secret key negotiation response message after encryption using the common key of MT or AP; and

3) After it receives said secret key negotiation response message from AP or MT, MT or AP, uses its own private key for decryption, obtains the random data generated by the other part; both MT and AP utilizes the random data generated by the other part and itself to generate the secret key for conversation.

20. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 1, 2, 3, 5, 6 or 7, wherein: said negotiation of secret key for conversation comprising:

1) MT or AP generates a string of random data, and, after it utilizes the common key of AP or MT for encryption, attaches its own signature as the secret key negotiation request message, and transmits it to AP or MT; and

2) after AP or MT receives said secret key negotiation request message from MT or AP, it utilizes the common key of MT or AP to authenticate the signature, and then utilizes its own private key to decrypt the encrypted message received; both MT and AP uses the random data as the secret key for conversation.

21. The method for the secure access of mobile terminal to the Wireless Local Area Network (WLAN) and for secure data communication via wireless link according to claim 17, 18, or 19, wherein: said negotiation of secret key for conversation possibly also comprising negotiation of the communication algorithm used in the process of communication.